REPORT ON INTERROGATION OF
KOMMANDEUR DER NACHR. AUFKL. 1 (KONA 1)
AT REVIN, FRANCE, JUNE 1945

ANNEXE 1

(REPORT ON RUSSIAN CIPHERS)

* * * * *

TICOM
29 June 1945

Copy No. 16
No. of Pages 15

Distribution:

British
1. Director
2. D.D.3.
3. D.D.4.
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.) (2)
9. Lt.Col. Leathem

TICOM
10. Chairman
11-12. S.A.C. (2)
13. Cdr. Bacon
14. Cdr. Mackenzie
15. Cdr. Tandy
16. Lt.Col. Johnson
17. Lt.Cdr. Manson
18. Major Seaman
19. Lieut. Eachus
20. Lieut. Vance
21. Capt. Cowan
22. Lieut. Fehl
23-25. TICOM Files (3)

U.S.
26-27. CP-20-G (2) (via Lt. Pendergrass)
28. G-2 (via Lt. Col. Hilles)
29-30. S.S.A. (2) (via Major Seaman)
31. Director, S.I.D. ETOUSA (via Lt. Col. Johnson)

Additional
32-34. Lt.Col. Pritchard (3)

Report on Russian Ciphers.

Based on:

1) "Uebersicht der Russischen Chi-Verfahren (Nov. 1940 - Mai 1945)", by Ltn. Harry LOEFFLER (Feste Nachr. Aufkl. Stelle 10). (TICOM I-3)

2) Interrogation of LOEFFLER.

3) "N.K.W.D Codes" by Obergefr. G. THOMAS (Nachr. Aufkl. Ausw. Stelle 1).

4) Interrogation of THOMAS.

Table of Contents

(abridged headings).

A. Two-figure ciphers.

As a result of statements made by prisoners from German Close range Sig. Int. units to the Russians the use of two-figure ciphers by the Russians practically ceased from the end of 1943. Up to then they had been used as follows:-

In the period 1940 - 42 two-figure ciphers were far more used than all other ciphers put together. The most used was the PT-39 (Peregowornaä Tablica). It consisted of a square 10 x 10 giving 100 groups with or without alternative meanings, see Fig. I.

The alphabet lay in three columns, the figures 1 to 0 in one column, the remainder of the square consisting of words or phrases such as CO, Chief of Staff, Wireless Station, "we are changing to frequency....." etc. The latter groups had alternative meanings consisting of such phrases. In order to differentiate the two meanings the first column contained two groups,one meaning "Read letter" and the other "read words". Example of a two-figure message: (S.D.= Rifle Division)

17	86	CO	80	37		32	56
Read Words,Kommandeur		3	6	Read letters		S	D etc.

The recipher was carried out by means of a 10 x 10 Latin Square (i.e. no figure repeated in any one column or line). A line (or a column) of this square was allotted to each day of the month

Ex: 7th, 12th, 19th, 28th May Line A

1st, 9th, 13th, 29th May Line G

3rd, 6th, 10th, 19th May Column E

The recipher of the bigrams 17, 86, 00, 80 on 7thMay would according to Figure I be 10, 54, 99, 59.

PT-39 was used in the Army by Army Groups, Armies, Corps and Divisions and in the Air Force by Corps, Divisions and Regiments. The identification of the Latin Square used enabled the Germans to establish to which Front or Army the wireless station using it belonged, or as to whether it was an Army or Air Force Station.

The recipher rows (or columns) were first broken singly and then put together in the Latin Square,bearing in mind the area in which it was being used. Since the squares were often used for several months, the reconstruction of the squares was easily checked.

Recipher rows (or columns) could always be solved with a minimum of 15 - 20 groups.

Messages were of a technical signal or tactical nature, the latter more especially after the beginning of the Russian campaign in June 1941. From then on these messages gave many place-names, names of officers, etc. which were very useful.

This cipher was used from the extreme South to extreme North of the Front and in the back areas as far back as the CAUCASUS, Middle ASIA and North PERSIA. It was superseded in May 1942 by PT-42. This was similar to PT-39

See Fig. II.

The recipher method was the same as for PT-39. The solution of a row (or column) now required about 30 groups. PT - 42 was used by the Army and according to the instructions its use was restricted to Army Groups, Armies and Corps. For Divisions and Regiments PT-42N was used. It was smaller, being only 7 x 10 instead of 10 x 10. See Fig. III.

Its construction was the same as PT-42. It was re-enciphered by means of rows as before but these were scarecely ever derived from a Latin Square. It was used almost exclusively from Division forwards and produced much tactical information; it remained in force in some cases until 1944. Solution of recipher rows was easier than with PT-42 owing to the basic code being smaller and to there being fewer alternatives to the letters.

Simultaneously with the introduction of PT-42, the Air Force introduced a similar 2-figure cipher. Its Russian designation was unknown to the Germans who called it R2ZC 781. The only difference between it and PT-42 was in the placing of the letters of the alphabet. The recipher was by means of a Latin Square.

It was possible from now on to establish whether a wireless station belonged to the Army or the Air Force by the cipher used.

At the same time the Air Force, especially the ground organisation but also individual Air Divisions, started using a variety of special 2-figure ciphers. These continued in different forms up to the last. These were either without alternatives with the letters of the Alphabet distributed over 4,5,6,7 or 8 columns and correspondingly fewer rows, or with alternatives and with the arrangement of the letters varying a great deal from one code to another.

Small independent special units such as Pionier Brigades, Mortar Regiments and Artillery Brigades, had their own home-made 2-figure ciphers which were often in use for only short periods and which, besides the letters of the Alphabet and numbers, contained specialised expressions appropriate to the unit concerned.

PT-42 was superseded by PT-43 which was the last general code used and was in force up to the capitulation. It contained no letters and was used for addresses, particularly by the Air Force and P.W.O. (A.A.defence).

B. Three-Figure Ciphers.

Three-figure ciphers were first noticed in February 1941. They were used increasingly from May 1941 and the beginning of the Russian Campaign. From then until the second half of 1942, the Air Force were the greatest users of this cipher and each Air Division had its own cipher. In 1942 the first Army unit (the 46th Army then in the CAUCASUS) started using a three-figure syllabic code.

By the time of STALINGRAD practically every Army engaged in the battle had its own 3-figure cipher.

The first 3-figure ciphers were very simple in form. They consisted of several pages (at most 10) and contained

(alphabetically semi-hatted, or completely "hatted") the numbers 1 to 0 and punctuation marks. See Fig. IV.

Soon afterwards the letters of the alphabet were put in their alphabetic position in the book. See Fig. V.

After some months the strictly alphabetic nature of the books was given up and the alphabeticity only maintained within the area of a letter. The numbers were at the same time distributed at random over the pages. See Fig. VI.

Besides the above types of codes, syllabic codes were used which contained few words but practically all the possible syllables which could be formed out of two or three letters. All codes of this kind which were broken were alphabetic. See Fig. VII.

From the beginning of 1943 most 3-figure codes no longer contained single letters but used the initial letter of the words for this purpose. In order to indicate which meaning was to be used two groups were introduced:

736 1) Read the initial letter

737 2) Read the whole word.

The three-figure groups were read in the order of page-line.

The recipher of three-figure ciphers was as varied as in the case of two-figure ciphers. Each figure was re-enciphered separately. That is to say, for the page numbers a hatted order of the figures 1 to 0 was substituted. Thus
Page 1 became 4
" 2 " 6
" 3 " 8 etc. See Fig. VIII.

The same was done for each figure of the lines with a different order of figures used for the substitution in each case.

The substitutions for the figures of the lines could be different on every page or it could be the same. The substitutions could be constructed without any recognisable system or they could be made up from a Latin Square. In the latter case the system used was as follows.

A starting point was chosen in the Latin Square (See Fig. I) say the 9 in Row B, the substitution row could then be formed by reading to the right of this point, or the left, or up, or down, or even by taking every other figure in any of these directions (the actual method to be used was laid down in the instructions issued with the cipher). This was done for each figure of the 3-figure group. The starting point in each case was indicated by its coordinates, i.e. 9 in Row B would be 25. The three pairs thus formed were then combined into a six figure group which was then divided into two three-figure groups which were either placed at the beginning or end of the message. A Latin Square usually lasted about a month though in the Air Force it sometimes lasted longer.

If a code was smaller than the possible 1000 groups, alternatives could be given to either the pages or the first figure of the lines. For example if the code only had five pages. Page 1 = 0 and 8
2 = 3 and 6

The first figure of the lines could have as many as three alternatives. The size of the codes used was in fact extremely varied, anything from two to ten pages.

Three-figure ciphers were used by the Army Groups, Armies, Corps and Division for strategic and tactical reports as well as for supply and personnel matters.

Every Army Group, Army, Corps, Division, Brigade, Regiment, Abteilung had its own 3-figure cipher which it used to its subordinate units. Similarly it was possible for one unit to use different ciphers for different subjects, i.e. one cipher was used from January to May 1945 by the 3rd Guards Tank Army for 1(a) reports and another for 1(c).

Air Force ciphers were often current for much longer periods than was the case with the Army and were known to last for more than a year. Army ciphers were nearly always changed after a big operation and were with few exceptions never current for more than a month or two, and sometimes for only a few weeks.

This type of cipher ended in 1943 and was superseded by three-figure Signal Codes.

They contained no letters but only words and phrases of tactical import. They were not alphabetic but the meanings were grouped under various headings such as 1st Group "Attack", 2nd Group "Defence", 3rd Group "Supply", 4th Group "Enemy movements", 5th Group "Designations of Units", 6th Group "Figures and numbers", 7th Group "Signal connections" etc. Each meaning had two or three three-figure groups allotted to it. Anything not contained in the code was sent "en clair". Messages also contained a lot of Coordinates. Messages in a Signal Code often contained the letter Alpha or é in the preamble or an indicator of the form 111, 222, 555, 777 or something similar. Every unit from Army downwards had its own Signal Code which it used to its subordinate units. See Fig. IX.

Three-Figure Address Codes.

These codes were used in connection with 5-Figure messages to enable wireless stations to ensure that messages arrived at their proper destination. Their construction was similar to that of the PT-39 or PT-42 but they contained only figures, unit designations, authorities, words such as "for" or "from". See Fig. X.

Example of an address:

783 625 825 824 017 389 930 837 401

For Cipher Branch 5th Army from 4 Guards Tank Corps

A code of this type was first used at the beginning of 1944 on the 1st & 2nd Ukrainian and 1st White Russian Fronts for communications between the Army Groups and their respective Armies and independent Corps. In the summer of 1944 armies began to use similar codes with their subordinate units and latterly the use of such codes increased still further.

The solution of these codes, given a fair amount of material, was generally easy. They were often simpler than the example given in Fig.X and sometimes appeared in the form of straightforward lists with each meaning numbered consecutively.

of 100 pages instead of 10. See Fig. XI.

The same variations in construction occur as with three-figure

1) Alphabetic with the letters of the alphabet grouped at the end of the Code.

2) Each letter of the alphabet placed before the part devoted to words beginning with that letter.

3) Semi-hatted, i.e. with all the words beginning with one letter grouped together but the groups in random order.

4) Letters of the alphabet with alternatives.

5) Syllabic Codes (with words distributed over the code).

6) Without letters of the alphabet but with the groups
(a) Read initial letter
(b) Read the word.

7) With the groups (a) and (b) above appearing several times, often on each page.

Codes had anything from 5 to 100 pages. The Air Force Codes usually had about 10,000 groups and the Army 5,000 or less.

The method of Reciphering was still more varied than in the case of three-figure ciphers.

1) For each figure of the four-figure group a substitution row could be used. See Fig. XII.
This form of recipher first appeared in September 1943 and was used by the Tank Supply and Administration authorities of the Don front.

2) Bigram substitution could be used. See Fig. XIII.

3) (1) and (2) above could be combined, and the first pair of the 4-figure group was reciphered by means of a bigram table and the last pair singly, or vice-versa.

4) If the basic code was less than 10,000, alternative figures could be used in the recipher as in Fig. XIV which is an actual example of the recipher used by the Tank Supply and Administration Authorities of the 1st Ukraine Front from February - March 1945. See Fig. XIV.

The code in question was 5 x 5 x 5 x 4 = 500 groups.

A general Army 4-figure cipher was last observed in use in North PERSIA in the winter 1941 - 42. It had 50 pages each designated by two alternative bigrams and 100 lines to each page. It was the forerunner of the 5-figure ciphers. From May 1941 the Air Force began to use four-figure ciphers of many different forms but often of the simplest construction. In the middle of 1943 many mobile formations, Tank and Mechanised Corps, Tank Armies and Tank Administration and supply units started using this type of cipher. As was the case with 3-figure ciphers, every independent formation had its own cipher for use with its subordinate units.

From 1944 four-figure Signal Codes made their

Four-figure ciphers were also used by Railway and Transport nets.

Generally speaking 4-figure ciphers were changed less frequently than other ciphers.

1) Four-Figure Cipher used by VI Guards Mech: Corps (1st Ukraine Front) from January 1945 to the end of hostilities. (It was captured in January 1945).

The notes that follow refer to model No.1.

Size.

5 pages, 6 columns and 20 lines on each page. The order of reading a group was A = Page, B = Column, CD = Line. This book contained only words and numbers, no single letters or syllables.

Recipher.

Three strips are used for this recipher. One containing the recipher of the page and columns is laid along the bottom. The other two are laid on either side of the book. The one used on the left hand side contains the numbers 00 to 49 and the one on the right those from 50 to 99. There are ten of each category of strip available and each of the ten is designated by a number from 0 to 9 chosen at random. The strips being used care indicated by a four-figure group placed at the beginning and end of the message. The first figure of this group is the figure allotted to the bottom strip, the second figure is that allotted to the strip on the left hand side and the third the one on the right. The fourth figure is a dummy. Thus in the example given on the attached model the indicator would be 952(6).

The strips were usually changed after about a fortnight.

It will be seen that the word RADIO could be represented by 24 different groups in the example given.

The names of places or words which did not appear in the Code book were spelt out by means of the initial letters of words in the code book, the group CB (letters follow) being inserted before beginning to spell and the group CC (words follow) at the end of the spelling. It will be seen that there are up to 1000 groups for any one letter.

Every Code captured had a Russian designation of the following form.

1) PT 403 A (Army)
2) PT 403 K (Corps)
3) PT 403 B (Brigade)
4) PT 403 D (Division)

1) would be used from Army to Corps
2) " " " Corps to Brigade
3) " " " Brigade to Regiments
4) " " " Division to Regiments.

2) Four-Figure Cipher of the 152 Independent Tank Brigade (60th Army 1st Ukraine Front).

The notes that follow refer to Model No.2.

can be used in conjunction with each page of the code book. The 4-figure group representing a word in the Code book is read off in the order A B C D shown on the model. Thus RADIO could be 5641 etc. The Indicator shows which strip is being used with which page. The first figure indicating the strip used with page 1, the second that used with page 2, and the third that used with page 3. The last is a dummy. It will be seen from the model that, there being six strips and ten figures available for their indication, four of the strips can have alternative indicator figures.

The code book was current for several months but the series of strips was changed either fortnightly or monthly according to instructions.

3) Signal Code of the VI Guards Tank Corps (3rd Guards Tank Army 1st Ukraine Front).

The notes that follow refer to Model No.3.

The code consisted of ten columns and eighteen lines. The recipher was carried out by means of horizontal and vertical strips consisting of bigrams. Thus RADIO could be represented by 0119 etc. in the example shown. There were ten strips of each type, each of the ten was designated by a number of consecutive bigrams i.e. 00 to 11 or 12 to 19 etc. The strips being used were shown by a 4-figure indicator group the first pair of which represented the horizontal strip and the second, the vertical strip.

4) Four-Figure Cipher of the Tank Supply and Administration Authorities of the 1st Ukraine Front.

The notes that follow refer to Model No.4.

The code book was used from February 1945 until the end of hostilities. During this time ten alternatives for each of the three reciphering strips were used. The figures representing a word in the book were read in the order Elements D A B C shown in the model. Thus RADIO could be represented by 3751 etc. Each of the ten strips was designated by one of the figures 0 - 9. The indicator was the 2nd Group (and often the last group of the message). The first figure indicated the strip used for Element D, the second Element A and the third and fourth Element BC of the model i.e. 6756 in the example shown.

5) Four-Figure Cipher used by the 76th Regional Air Base (Russian: - 76 RAB).

The notes that follow refer to Model No.5.

The cipher was current from May 1944 until the end of hostilities.

The Code Book consisted of 40 columns and 40 lines. The columns had two bigrams each allotted to them, the lines only one, the bigrams ran consecutively in each case. It contained single letters, numbers, syllables, words, types. It did not contain the groups "Read initial letter", "Read words". Reciphering was carried out by means of three adjacent bigram tables. No indicators as such were used but a full stop always occurred in the second and last place of the message which enabled the recipient to tell which table

The notes that follow refer to Model No.6.

The cipher was current from February 1945 until the end of hostilities.

This cipher was not completelybroken by the Germans and they were uncertain about various points. The indicator group was placed at the beginning and end of the message. Its first pair probably indicated the vertical recipher strip used and the second the horizontal. The recipher was probably carried out by bigram substitution. Various methods of reciphering were current at the same time.

7) Cipher used by 3rd Guards Tank Army.

The notes that follow refer to Model No.7.

Messages in this cipher first appeared on 15.1.45. The group 6666 always appeared at the beginning and end of messages and was probably a Code number. The second and penultimate groups of the message were the indicator, the first and third figures of which gave the pages to be used in the recipher, the second and fourth were dummies. Clear text, coordinates and signatures en clair appeared in the messages. Place names and signatures were seldom spelt out in cipher.

From 15.1.45 until the middle of March four reciphers were used concurrently, from the beginning of April only one.

The Code consisted of double pages A1, A2 and B1, B2 from which only two single pages were used at once i.e. A1 and A2 or A1 and B1 or A1 and B2 etc. In the example given the indicator 5033 shows that B1 and B2 are the pages used.

Example:

6666	5033	5432	0331	1392	37582
Code Nr.	Indicator.	PROTIWN	WEDEJBOI	ÜVNEE	Co-ordinates

3348 UNIÕTOVENO etc.

D. Five-Figure Ciphers.

Five-figure Code books contained about 25,000 out of the possible 100,000 groups, the pages being numbered 000 - 999 with a hundred lines on each page. The Germans never broke a book and any examples they had were captures.

The books were alphabetic at first but then became "semi-hatted" i.e. all groups with the same initial letter were grouped together but not alphabetically, nor were the initial letters alphabetic with reference to one another.

The books contained

1) Single letters

2) Words

3) Phrases

4) Two-figure numbers

7) Full stops and commas on every page.

8) All designations of types, such as Types of Tanks, ammunition, wireless stations, transport etc. I 19

Five-figure ciphers were used both by the Army and Air Force as follows.

(a) Army

N.K.O. (Defence Council)
Army Groups
Armies
Corps
Divisions
Brigades

(b) Air

Air Armies
Air Corps
Air Divisions
R.A.B. (Air Ground Regions)
P.W.O. (A.A.Defence)
A.A. Corps
A.A. Divisions.

The messages contained strategic, tactical, personnel and supply matters. Also political directives and reports.

Recipher.

KONA.1 did not deal with 5-figure traffic but sent it back to BERLIN. Prisoners statements on the subject of the method of recipher used were therefore somewhat confused but it is thought that the following represents the true picture as far as they knew it.

An additive was used for the recipher. This consisted of pads known as BLOCKNOTS which contained a variable number of sheets on which were printed anything from 50 - 100 5-Figure groups. Each pad was given a five-figure number and each sheet of the pad a two-figure number which ran consecutively. There were five different types of BLOCKNOT.

1) I (INDIWIDUALNY) known by Figure 3.
2) Z (ZIRKULARNY) " " 6.
3) OS (?) " " 2.
4) NOTBLOCK(emergency Block) " " 1
5) A BLOCKNOT used for passing on traffic. " " 8

BLOCKNOTS I contained 50 pages and were used in one direction only.

BLOCKNOTS Z & OS contained 30 pages and could be used in either direction.

The distribution of BLOCKNOTS was carried out centrally from MOSCOW - Army Groups - Armies. The Army was responsible for their distribution throughout the lower levels. Independent units always took their cipher material with them and one case occurred of a unit being silent for nine months and then being heard using the same series of BLOCKNOTS

Occasionally the same BLOCKNOT was distributed to two units on different parts of the front with the result that a depth was established. Records of all BLOCKNOTS used were kept in BERLIN and when a repeat was noticed a "BLOCKNOT ANGEBOT" was sent out to all German S.I. units. It seems that depths of up to 8 were established at the beginning of the Russian Campaign but that no 5-figure was broken after May 1943.

Prisoner stated definitely that each of the figures 0 - 9 occurred the same number of times on any one page of a BLOCKNOT and that if a count of the figures in the cipher text was made the frequency of each figure always lay between 9 and 11%.

The two indicators of the BLOCKNOT were placed en clair usually within the first ten groups of the text or sometimes at the end. One indicator was the BLOCKNOT number and the other consisted of two random figures, the figure representing the type, and the remaining two the page of the BLOCKNOT being used.

In long messages 00000 was placed in the message when the end of a page had been reached.

E. Four-letter Ciphers.

Two forms of four-letter cipher first appeared in practice traffic between Army Groups and Armies and independent Corps of the 1st Ukraine Front in November 1944.

1) Revolving Stencil.

This consisted of a sheet of paper ruled off into 8 x 8 squares. On top was placed another sheet in which 16 holes were cut of corresponding size to the squares on the first sheet. These holes were so cut that if the sheet is turned through 90° round the centre point in the four possible positions and a letter written on the bottom sheet through each hole in each position , all 64 squares on the bottom sheet would be filled. The text of the message to be enciphered was written in the holes horizontally with the stencil in the first then in the second, third and fourth positions. The cipher text was then read off horizontally and sent in four letter groups. If a message was longer than 64 letters the process was repeated as many times as necessary.

The revolving stencil was changed from time to time.

2) Transposition.

This cipher is a simple transposition cipher, the key being given by a Keyword and the text being written in vertically according to the key and either upwards or downwards according to accompanying instructions. The cipher text was then read off horizontally and sent in 4 or 5-letter groups. See Fig. XVI.

The contents of messages sent in both the above types of cipher were usually about technical signal matters though recently units and positions were named.

F. Word Code.

It consisted of two halves each of which was designated by a word such as SEWER ZAPAD. The clear groups such as numbers, units, offices, designations such as Tank, Guards, Mechanised etc. were grouped in two columns. Each half of the code contained a number of columns with cover-words.

The first half of the code is used with column 1 and the second half with column 2. The order of the halves can be changed and indicated by the indicating word.

If the clear group consists of more than one word such as "In the former sector " = Dolvnost and the wanted word is "former ", this can be indicated by saying "the second word of" DOLVNOST. See Fig. XVII.

Example: MOLNIA POZDNO REMONT KTO PAKET

1a 3 Guards Tank Army.

The codes identified were only used by the Army and contained strategic and tactical reports and the names of units. They were small in size and contained only essential groups. Anything that could not be enciphered was sent in clear. Coordinates also appeared in messages,

G. Miscellaneous.

1) Coordinate Systems.

These were very varied. Armies made up their own systems and arbitary reference points and grids were used.

2) Codenames.

These were always changed before an offensive. They tended to be systematic within a particular branch of the Army.

H. General Remarks on Section I (Army and Air).

In the above paper examples are given only of those ciphers whose basic construction was established. There were many types of cipher which were only partially broken and whose basic form could not be established, these are not mentioned. A number of ciphers were later captured and the German results confirmed. Other captures enabled them to read ciphers currently.

The original Russian designation of a particular cipher was in most cases unknown and a German designation was then given in the form R2ZC 706.

R = Russian, 2Z = Type, C = Code, 706 = Serial number. (Z=Ziffer = figure)

The number of Russian ciphers of all sorts that were broken was about 3000.

II N.K.W.D. Codes.

A. Five-Figure Ciphers.

These were not dealt with by KONA.1 but prisoner stated that 40 - 50 men were employed by LNA at ZOSSEN on the exploitation of such ciphers. He thought that a good deal of success was obtained in the case of Far Eastern Traffic. An additive was used for the recipher.

B. Four-Figure Ciphers.

The ciphers of the above type exploited by KONA.1 were used by front line units (Regiments and Battalions) of the N.K.W.D. These units were mainly employed as Military police.

Only one code book (known to the Germans as R 4 Z C 1800 and to the Russians as KODOWAA TABLICA "ZERNO") was used by the N.K.W.D. from October 1943 - end of 1944. It was used from Battalion upwards to Front HQ's, from Front HQ's upwards five-figure ciphers were used.

A model of the cipher and an example of an enciphered text are attached. The following notes refer to this Model and example. (See Model 8).

The book consisted of 50 pages each with two columns of 25 lines - 2500 groups in all. The book was alphabetic (the example made up by prisoner does not agree with this statement).

The recipher consisted of two elements.

1) Chiffrant

2) Bigram substitution tables.

1. The "Chiffrant" consisted of the figures 0 - 9 in random order printed at the top of each page, a different order being used for each page. The third figure of the four-figure indicator group gave the number of the chiffrant to be used, i.e. if 5 was the 3rd figure of the indicator group, the fifth figure of the "chiffrant" reading from left to right would be the one used for each page. This number was then added to the numbers of the lines on the page before they were reciphered by means of the bigram table. i.e. if the number was 6 then line 00 would become 06 and line 24 would become line 05.

2. Two different bigram substitution tables were used for reciphering the bigram representing the page and that representing the line. Ten such tables were in use concurrently for the recipher of both page and line. Each table was 10 x 10 so that each bigram could be reciphered in two different ways and each table was designated by one of the figures from 0 - 9. The figure designating the table used for the line was put in the second place of the indicator group and that designating the table used for the page in the fourth place. The first place was a dummy. A series of substitution tables was current for a period of from two to six months.

The indicator group was inserted en clair in one of the first ten groups of the message according to instructions. The penultimate group consisted of the date and length of the message and the last group the Chi number.

From 1933 - 42 R4ZC4 was in use. It consisted of a 100 page alphabetic book each with a hundred lines. Recipher was carried out by means of 31 bigram tables. It was broken by the Germans in 1940.